The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/12/2016

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in iOS, tvOS, and watchOS which could allow for arbitrary code execution. iOS is a mobile operating system for mobile devices, including the iPhone, iPad, and iPod touch. tvOS is an operating system for the fourth-generation Apple TV digital media player. watchOS is the mobile operating system of the Apple Watch and is based on the iOS operating system. Attackers can exploit these vulnerabilities to bypass security restrictions, execute arbitrary code and perform unauthorized actions or obtain sensitive information.

Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user, arbitrary code execution within the context of the application, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:
- iOS Versions prior to 10.2
- tvOS Versions prior to 10.1
- watchOS Versions prior to 3.1.1

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in iOS, tvOS, and watchOS. The most severe of the vulnerabilities could allow for arbitrary code execution. Details of all vulnerabilities are as follows:

- An information-disclosure vulnerability that affects the 'Accessibility' component. Specifically, this issue occurs in the handling of passwords (CVE-2016-7634).
- A security-bypass vulnerability that affects the 'Accessibility' component. Successful exploits may allow an attackers to access photos and contacts from the lock screen (CVE-2016-7664).
- A security-bypass vulnerability due to a state management issue. Specifically, this issue affects the 'Find My iPhone' component (CVE-2016-7638).
- A denial of service vulnerability because it fails to properly sanitize user-supplied input. Specifically, this issue affects the 'Graphics Driver' (CVE-2016-7665).
- An arbitrary code-execution vulnerability because it fails to properly handle USB image devices. Specifically, this issue affects the 'Image Capture' component (CVE-2016-4690).
- A security vulnerability that occurs due to a logic issue exist in the handling of the idle timer when the Touch ID prompt is shown. Specifically, this issue affect the Local Authentication (CVE-2016-7601).
- A security-bypass vulnerability that affects the 'Mail' component. Specifically, this issue occurs because S/MIME policy failed to check if a certificate was valid (CVE-2016-4689).
- A security-bypass vulnerability that affects the 'Media Player' component. Successful exploits may allow an attackers to view photos and contacts from the lockscreen (CVE-2016-7653).
- A security-bypass vulnerability that affects the 'SpringBoard' component. Specifically, this issue occurs in the handling of passcode attempts when resetting the passcode (CVE-2016-4781).
- A security-bypass vulnerability that affects the 'SpringBoard' component (CVE-2016-7597).
- A memory corruption vulnerability which by opening a maliciously crafted certificate may lead to arbitrary code execution (CVE-2016-7626).
- A security-bypass vulnerability which does not reset authorization settings on app uninstall (CVE-2016-7651).

Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user, arbitrary code execution within the context of the application, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:
Apple:
https://support.apple.com/en-us/HT207422

https://support.apple.com/en-us/HT207425
https://support.apple.com/en-us/HT207426

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4689
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4690
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4781
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7597
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7601
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7626
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7634
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7638
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7651
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7653
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7664
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7665